Defense Security Service
Industrial Security Field Operations
NISP Authorization Office

Technical Assessment Guide for Red Hat Enterprise Linux 6 OS

May 2016

Revision Log

Date	Revision	Description of Change
2016APR07	1.0	Initial Draft
2016MAY02	1.1	Updates to format, landscape tables, added “Notes” Section

Table of Contents

1.0 Tools and Documentation

Assessment of the technical security controls and system configuration of contractor Information Systems (IS) utilizing the Defense Information System Agency (DISA) vulnerability scanning protocols in accordance with the NISP will require the following tools and documentation:

1.1 Tools

Install these tools on the system to be scanned, or on a dedicated system for centralized (network) scanning.

1.1.1 SCAP Compliance Checker

A. The ISSP/SCA will verify the following parameters:

   1) Verify that the SCAP Compliance Checker is properly installed on the system that will conduct the vulnerability scan.
   2) Ensure that the latest version of the SCAP Compliance Checker is used. *Consult DISA's IASE website to validate the version of the SCAP Compliance Checker.*
   3) Ensure that the individual conducting the scans has administrator credentials for the host machine, as well as any client machines scanned across the network (if applicable). *For the purposes of network scanning, either domain-level administrator credentials or a local administrator account on the remote system is acceptable.*
   4) Verify that the ISSM/ISSO has selected the most recent appropriate Operating System benchmark within the ***Edit → Content and Options*** menu (e.g. *U_RedHat_6_V1R10_STIG_SCAP_1-1_Benchmark*).
      - The ISSP/SCA should verify on DISA's IASE website that the most recent benchmark is loaded.
      - If the most recent benchmark is not loaded into the SCAP Compliance Checker, instruct the ISSM/ISSO to manually download and import the most recent DISA benchmark.
      - Select only one benchmark (the most recent) for the scan operation.
   5) Verify that the ISSM/ISSO has set the SCAP Content Profile within the ***Edit → Content and Options*** menu for the selected benchmark to "***MAC-3 Classified***".

B. The ISSP/SCA will then instruct the ISSM/ISSO to execute the vulnerability scan of the system.

C. Upon completion of the scan, the ISSP/SCA will instruct the ISSM/ISSO to retrieve the XCCDF Scan Results XML file, for import into the STIG Viewer. Unless the user has changed the repository directory manually, the XCCDF Scan Results file can be located by navigating to ***Results → Open Results Directory*** in the SCAP tool menu.

1.1.2 DISA STIG Viewer

A. The ISSP/SCA will do the following:

1) Confirm that the DISA STIG Viewer (Version 2.3) is downloaded to a known directory.
2) Confirm that the ISSM/ISSO has downloaded the most recent Operating System baseline from the DISA IASE website.

B. Have the ISSM/ISSO import the recent baseline into the STIG Viewer, and create a checklist from the STIG baseline that includes all STIG vulnerabilities included within the baseline.

1.2 Documentation

Assessment of the technical system security controls and security configuration requires that the ISSP/SCA make risk-based decisions regarding compliance condition based on the approved/submitted plan. To facilitate the assessment the following documents will be reviewed by the ISSP/SCA:

A. Master System Security Plan (MSSP) and/or System Security Plan (SSP)
B. Authorization Letter (if performing a SVA)
C. Information System Profile (IS Profile)
D. Hardware and Software Baselines
E. Authorized Users List and Signed User Briefings
F. Trusted Download Procedures, Briefings and Logs
G. Risk Acceptance Letters (if applicable)
H. System Diagram and/or Network Topology (if applicable)
I. DD Form 254
J. DSS Form 147
K. MOU/ISA's (if applicable)
L. Manual Audit Log
M. Removable Media Creation Log
N. Maintenance Logs
O. Sanitization Procedures (if applicable)
P. Audit Variance/Hibernation Procedures (if applicable)

2.0 Assessment Procedures

In order to determine the compliance condition of the system, the ISSP/SCA along with the ISSM/ISSO will conduct the following steps:

1) Instruct the ISSM/ISSO to:
    a. Navigate to the "Checklist" tab within the STIG Viewer window.
    b. Navigate to the top menu of the STIG Viewer and click **Import → XCCDF Scan Results**.
    c. Navigate to the directory containing the SCAP Compliance Checker XML file
    d. Import the scan results.

    e. In the “Target Data” drop down, select the appropriate computing role (e.g. Workstation).
    f. In the “Technology Area” drop down, select “UNIX OS”.

2) The ISSP/SCA will then conduct the assessment to determine satisfactory implementation of the baseline technical standards:
    a. The ISSP/SCA may use the “CAT I/CATII/CATIII” tabs under the “Totals” dropdown to sort the vulnerabilities if desired. **The CAT severity levels provide a means by which to prioritize addressing of vulnerabilities; however, the severity levels should not be used in the vulnerability citing language. Citing of any vulnerability will refer to the associated RMF control (e.g. AU-12).**
    b. Sort the vulnerabilities by Vulnerability ID to allow for the efficient identification of the RMF control addressed by the selected Vulnerability ID (optional).
    c. Reference the **Control/Vulnerability ID Assessment Matrix** in **Appendix A** to determine the RMF control that is applicable to the open vulnerability. This RMF control information is also contained within the “CCI” tab of each vulnerability for ease of access.
    d. Consult the System Security Plan and any associated or supporting documentation to determine if the control is satisfactorily implemented, mitigated, tailored out, or non-compliant (open).
    e. Record any open vulnerabilities, follow-up or mitigation actions, and POAM’s (if applicable).

Appendix A – Control/Vulnerability ID Assessment Matrix/Checklist

The below matrix can be used to reconcile RMF controls with SCAP/STIG Vulnerability ID’s.

Legend:

- **Control ID**: NIST 800-53 Rev 4 RMF Control Identifier
- **Vuln. ID**: STIG Vulnerability Identifier
- **O**: OPEN Vulnerability (Non-Compliant)
- **M**: Open Vulnerability, Mitigated (Compliant)
- **C**: CLOSED Vulnerability (Compliant)
- **N/A**: Tailored Out in Plan, or Not Applicable to System Type (Compliant)
- **Description**: Short description of system setting and/or control requirements.

Control ID	Vuln ID	O	M	C	N/A	Description	Notes
AC-10	V-38684					The system must limit users to 10 simultaneous system logins or a site-defined number in accordance with operational requirements.	
AC-11 (1)	V-38639					The system must display a publicly-viewable pattern during a graphical desktop environment session lock.	
AC-11 a	V-38474					The system must allow locking of graphical desktop sessions.	
	V-38590					The system must allow locking of the console screen in text mode.	
	V-38629					The graphical desktop environment must set the idle timeout to no more than 15 minutes.	
	V-38630					The graphical desktop environment must automatically lock after 15 minutes of inactivity and the system must require user reauthentication to unlock the environment.	
	V-38638					The graphical desktop environment must have automatic lock enabled.	
AC-17	V-38444					The systems local IPv6 firewall must implement a deny-all allow-by-exception policy for inbound packets.	
	V-38491					There must be no .rhosts or hosts.equiv files on the system.	
	V-38513					The systems local IPv4 firewall must implement a deny-all allow-by-exception policy for inbound packets.	
AC-17 (1)	V-38631					The operating system must employ automated mechanisms to facilitate the monitoring and control of remote access methods.	
AC-17 (2)	V-38594					The rshd service must not be running.	
	V-38598					The rexecd service must not be running.	
	V-38625					If the system is using LDAP for authentication or account information the system must use a TLS connection using FIPS 140-2 approved cryptographic algorithms.	

AC-17 (8)	V-38602	🟥	🟨	🟩	▨	The rlogind service must not be running.	
	V-38609	🟥	🟨	🟩	▨	The TFTP service must not be running.	
	V-38673	🟥	🟨	🟩	▨	The operating system must ensure unauthorized security-relevant configuration changes detected are tracked.	
	V-38674	🟥	🟨	🟩	▨	X Windows must not be enabled unless required.	
AC-19	V-38490	🟥	🟨	🟩	▨	The operating system must enforce requirements for the connection of mobile devices to operating systems.	
	V-38655	🟥	🟨	🟩	▨	The noexec option must be added to removable media partitions.	
	V-38682	🟥	🟨	🟩	▨	The Bluetooth kernel module must be disabled.	
AC-19 c	V-38691	🟥	🟨	🟩	▨	The Bluetooth service must be disabled.	
AC-2 (1)	V-38439	🟥	🟨	🟩	▨	The system must provide automated support for account management functions.	
	V-38685	🟥	🟨	🟩	▨	Temporary accounts must be provisioned with an expiration date.	
	V-38690	🟥	🟨	🟩	▨	Emergency accounts must be provisioned with an expiration date.	
AC-2 (3)	V-38692	🟥	🟨	🟩	▨	Accounts must be locked upon 35 days of inactivity.	
AC-2 (4)	V-38531	🟥	🟨	🟩	▨	The operating system must automatically audit account creation.	
	V-38534	🟥	🟨	🟩	▨	The operating system must automatically audit account modification.	
	V-38536	🟥	🟨	🟩	▨	The operating system must automatically audit account disabling actions.	
	V-38538	🟥	🟨	🟩	▨	The operating system must automatically audit account termination.	
AC-3	V-38585	🟥	🟨	🟩	▨	The system boot loader must require authentication.	
	V-38586	🟥	🟨	🟩	▨	The system must require authentication upon booting into single-user and maintenance modes.	

	V-38588	🟥	🟨	🟩	⬜	The system must not permit interactive boot.	
AC-4	V-38616	🟥	🟨	🟩	⬜	The SSH daemon must not permit user environment settings.	
AC-6 (2)	V-38567	🟥	🟨	🟩	⬜	The audit system must be configured to audit all use of setuid and setgid programs.	
AC-7	V-38501	🟥	🟨	🟩	⬜	The system must disable accounts after excessive login failures within a 15-minute interval.	
	V-38592	🟥	🟨	🟩	⬜	The system must require administrator action to unlock an account locked by excessive failed login attempts.	
AC-7 a	V-38573	🟥	🟨	🟩	⬜	The system must disable accounts after three consecutive unsuccessful logon attempts.	
AC-8 a	V-38599	🟥	🟨	🟩	⬜	The FTPS/FTP service on the system must be configured with the Department of Defense (DoD) login banner.	
	V-38615	🟥	🟨	🟩	⬜	The SSH daemon must be configured with the Department of Defense (DoD) login banner.	
AC-8 b	V-38688	🟥	🟨	🟩	⬜	A login banner must be displayed immediately prior to or as part of graphical desktop environment login prompts.	
AC-8 c	V-38593	🟥	🟨	🟩	⬜	The Department of Defense (DoD) login banner must be displayed immediately prior to or as part of console login prompts.	
	V-38689	🟥	🟨	🟩	⬜	The Department of Defense (DoD) login banner must be displayed immediately prior to or as part of graphical desktop environment login prompts.	
AC-9	V-38484	🟥	🟨	🟩	⬜	The operating system upon successful logon must display to the user the date and time of the last logon or access via ssh.	
AU-12 a	V-38438	🟥	🟨	🟩	⬜	Auditing must be enabled at boot by setting a kernel parameter.	

	V-38521	🟥	🟨	🟩	▨	The operating system must support the requirement to centrally manage the content of audit records generated by organization defined information system components.	
	V-38522	🟥	🟨	🟩	▨	The audit system must be configured to audit all attempts to alter system time through settimeofday.	
	V-38525	🟥	🟨	🟩	▨	The audit system must be configured to audit all attempts to alter system time through stime.	
	V-38527	🟥	🟨	🟩	▨	The audit system must be configured to audit all attempts to alter system time through clock_settime.	
	V-38530	🟥	🟨	🟩	▨	The audit system must be configured to audit all attempts to alter system time through /etc/localtime.	
	V-38635	🟥	🟨	🟩	▨	The audit system must be configured to audit all attempts to alter system time through adjtimex.	
AU-12 c	V-38543	🟥	🟨	🟩	▨	The audit system must be configured to audit all discretionary access control permission modifications using chmod.	
	V-38545	🟥	🟨	🟩	▨	The audit system must be configured to audit all discretionary access control permission modifications using chown.	
	V-38547	🟥	🟨	🟩	▨	The audit system must be configured to audit all discretionary access control permission modifications using fchmod.	
	V-38550	🟥	🟨	🟩	▨	The audit system must be configured to audit all discretionary access control permission modifications using fchmodat.	
	V-38552	🟥	🟨	🟩	▨	The audit system must be configured to audit all discretionary access control permission modifications using fchown.	

	V-38554	🟥	🟨	🟩	⬜	The audit system must be configured to audit all discretionary access control permission modifications using fchownat.	
	V-38556	🟥	🟨	🟩	⬜	The audit system must be configured to audit all discretionary access control permission modifications using fremovexattr.	
	V-38557	🟥	🟨	🟩	⬜	The audit system must be configured to audit all discretionary access control permission modifications using fsetxattr.	
	V-38558	🟥	🟨	🟩	⬜	The audit system must be configured to audit all discretionary access control permission modifications using lchown.	
	V-38559	🟥	🟨	🟩	⬜	The audit system must be configured to audit all discretionary access control permission modifications using lremovexattr.	
	V-38561	🟥	🟨	🟩	⬜	The audit system must be configured to audit all discretionary access control permission modifications using lsetxattr.	
	V-38563	🟥	🟨	🟩	⬜	The audit system must be configured to audit all discretionary access control permission modifications using removexattr.	
	V-38565	🟥	🟨	🟩	⬜	The audit system must be configured to audit all discretionary access control permission modifications using setxattr.	
	V-38566	🟥	🟨	🟩	⬜	The audit system must be configured to audit failed attempts to access files and programs.	
	V-38568	🟥	🟨	🟩	⬜	The audit system must be configured to audit successful file system mounts.	
	V-38575	🟥	🟨	🟩	⬜	The audit system must be configured to audit user deletions of files and programs.	
	V-38578	🟥	🟨	🟩	⬜	The audit system must be configured to audit changes to the /etc/sudoers file.	

	V-38580	🟥	🟨	🟩	⬜	The audit system must be configured to audit the loading and unloading of dynamic kernel modules.	
AU-3	V-38628	🟥	🟨	🟩	⬜	The operating system must produce audit records containing sufficient information to establish the identity of any user/subject associated with the event.	
	V-38632	🟥	🟨	🟩	⬜	The operating system must produce audit records containing sufficient information to establish what type of events occurred.	
	V-38702	🟥	🟨	🟩	⬜	The FTP daemon must be configured for logging or verbose mode.	
AU-3 (2).1 (ii)	V-38471	🟥	🟨	🟩	⬜	The system must forward audit records to the syslog service.	
AU-4	V-38467	🟥	🟨	🟩	⬜	The system must use a separate file system for the system audit data path.	
	V-38470	🟥	🟨	🟩	⬜	The audit system must alert designated staff members when the audit storage volume approaches capacity.	
AU-5 (1)	V-38678	🟥	🟨	🟩	⬜	The audit system must provide a warning when allocated audit record storage volume reaches a documented percentage of maximum audit record storage capacity.	
AU-5 a	V-38680	🟥	🟨	🟩	⬜	The audit system must identify staff members to receive notifications of audit log storage volume capacity issues.	
AU-5 b	V-38464	🟥	🟨	🟩	⬜	The audit system must take appropriate action when there are disk errors on the audit storage volume.	
	V-38468	🟥	🟨	🟩	⬜	The audit system must take appropriate action when the audit storage volume is full.	
AU-8 (1)	V-38620	🟥	🟨	🟩	⬜	The system clock must be synchronized continuously or at least daily.	
	V-38621	🟥	🟨	🟩	⬜	The system clock must be synchronized to an	

		🟥	🟨	🟩	▨	authoritative DoD time source.	
AU-9	V-38445	🟥	🟨	🟩	▨	Audit log files must be group-owned by root.	
	V-38493	🟥	🟨	🟩	▨	Audit log directories must have mode 0755 or less permissive.	
	V-38495	🟥	🟨	🟩	▨	Audit log files must be owned by root.	
	V-38498	🟥	🟨	🟩	▨	Audit log files must have mode 0640 or less permissive.	
	V-38663	🟥	🟨	🟩	▨	The system package management tool must verify permissions on all files and directories associated with the audit package.	
	V-38664	🟥	🟨	🟩	▨	The system package management tool must verify ownership on all files and directories associated with the audit package.	
	V-38665	🟥	🟨	🟩	▨	The system package management tool must verify group-ownership on all files and directories associated with the audit package.	
AU-9 (2)	V-38520	🟥	🟨	🟩	▨	The operating system must back up audit records on an organization defined frequency onto a different system or media than the system being audited.	
AU-9 (3)	V-38637	🟥	🟨	🟩	▨	The system package management tool must verify contents of all files associated with the audit package.	
CM-5	V-38462	🟥	🟨	🟩	▨	The RPM package management tool must cryptographically verify the authenticity of all software packages during installation.	
	V-38476	🟥	🟨	🟩	▨	Vendor-provided cryptographic certificates must be installed to verify the integrity of system software.	
CM-5 (6)	V-38465	🟥	🟨	🟩	▨	Library files must have mode 0755 or less permissive.	
	V-38466	🟥	🟨	🟩	▨	Library files must be owned by a system account.	
	V-38469	🟥	🟨	🟩	▨	All system command files must have mode 755 or	

		🟥	🟨	🟩	⬜	less permissive.	
	V-38472	🟥	🟨	🟩	⬜	All system command files must be owned by root.	
CM-6 (2)	V-38695	🟥	🟨	🟩	⬜	A file integrity tool must be used at least weekly to check for unauthorized file changes particularly the addition of unauthorized system libraries or binaries or for unauthorized modification to authorized system libraries or binaries.	
CM-6 b	V-38437	🟥	🟨	🟩	⬜	Automated file system mounting tools must not be enabled unless needed.	
	V-38443	🟥	🟨	🟩	⬜	The /etc/gshadow file must be owned by root.	
	V-38446	🟥	🟨	🟩	⬜	The mail system must forward all mail for root to one or more system administrators.	
	V-38447	🟥	🟨	🟩	⬜	The system package management tool must verify contents of all files associated with packages.	
	V-38448	🟥	🟨	🟩	⬜	The /etc/gshadow file must be group-owned by root.	
	V-38449	🟥	🟨	🟩	⬜	The /etc/gshadow file must have mode 0000.	
	V-38450	🟥	🟨	🟩	⬜	The /etc/passwd file must be owned by root.	
	V-38451	🟥	🟨	🟩	⬜	The /etc/passwd file must be group-owned by root.	
	V-38452	🟥	🟨	🟩	⬜	The system package management tool must verify permissions on all files and directories associated with packages.	
	V-38453	🟥	🟨	🟩	⬜	The system package management tool must verify group-ownership on all files and directories associated with packages.	
	V-38454	🟥	🟨	🟩	⬜	The system package management tool must verify ownership on all files and directories associated with packages.	
	V-38455	🟥	🟨	🟩	⬜	The system must use a separate file system for /tmp.	
	V-38456	🟥	🟨	🟩	⬜	The system must use a separate file system for	

		🟥	🟨	🟩	⬜	/var.	
	V-38457	🟥	🟨	🟩	⬜	The /etc/passwd file must have mode 0644 or less permissive.	
	V-38458	🟥	🟨	🟩	⬜	The /etc/group file must be owned by root.	
	V-38459	🟥	🟨	🟩	⬜	The /etc/group file must be group-owned by root.	
	V-38461	🟥	🟨	🟩	⬜	The /etc/group file must have mode 0644 or less permissive.	
	V-38463	🟥	🟨	🟩	⬜	The system must use a separate file system for /var/log.	
	V-38473	🟥	🟨	🟩	⬜	The system must use a separate file system for user home directories.	
	V-38480	🟥	🟨	🟩	⬜	Users must be warned 7 days in advance of password expiration.	
	V-38496	🟥	🟨	🟩	⬜	Default operating system accounts other than root must be locked.	
	V-38497	🟥	🟨	🟩	⬜	The system must not have accounts configured with blank or null passwords.	
	V-38499	🟥	🟨	🟩	⬜	The /etc/passwd file must not contain password hashes.	
	V-38500	🟥	🟨	🟩	⬜	The root account must be the only account having a UID of 0.	
	V-38502	🟥	🟨	🟩	⬜	The /etc/shadow file must be owned by root.	
	V-38503	🟥	🟨	🟩	⬜	The /etc/shadow file must be group-owned by root.	
	V-38504	🟥	🟨	🟩	⬜	The /etc/shadow file must have mode 0000.	
	V-38511	🟥	🟨	🟩	⬜	IP forwarding for IPv4 must not be enabled unless the system is a router.	
	V-38523	🟥	🟨	🟩	⬜	The system must not accept IPv4 source-routed packets on any interface.	
	V-38524	🟥	🟨	🟩	⬜	The system must not accept ICMPv4 redirect packets on any interface.	
	V-38526	🟥	🟨	🟩	⬜	The system must not accept ICMPv4 secure redirect packets on any interface.	

	V-38528	🟥	🟨	🟩	⬜	The system must log Martian packets.	
	V-38529	🟥	🟨	🟩	⬜	The system must not accept IPv4 source-routed packets by default.	
	V-38532	🟥	🟨	🟩	⬜	The system must not accept ICMPv4 secure redirect packets by default.	
	V-38533	🟥	🟨	🟩	⬜	The system must ignore ICMPv4 redirect messages by default.	
	V-38535	🟥	🟨	🟩	⬜	The system must not respond to ICMPv4 sent to a broadcast address.	
	V-38537	🟥	🟨	🟩	⬜	The system must ignore ICMPv4 bogus error responses.	
	V-38540	🟥	🟨	🟩	⬜	The audit system must be configured to audit modifications to the systems network configuration.	
	V-38541	🟥	🟨	🟩	⬜	The audit system must be configured to audit modifications to the systems Mandatory Access Control (MAC) configuration (SELinux).	
	V-38542	🟥	🟨	🟩	⬜	The system must use a reverse-path filter for IPv4 network traffic when possible on all interfaces.	
	V-38544	🟥	🟨	🟩	⬜	The system must use a reverse-path filter for IPv4 network traffic when possible by default.	
	V-38546	🟥	🟨	🟩	⬜	The IPv6 protocol handler must not be bound to the network stack unless needed.	
	V-38548	🟥	🟨	🟩	⬜	The system must ignore ICMPv6 redirects by default.	
	V-38579	🟥	🟨	🟩	⬜	The system boot loader configuration file(s) must be owned by root.	
	V-38581	🟥	🟨	🟩	⬜	The system boot loader configuration file(s) must be group-owned by root.	
	V-38583	🟥	🟨	🟩	⬜	The system boot loader configuration file(s) must have mode 0600 or less permissive.	
	V-38596	🟥	🟨	🟩	⬜	The system must implement virtual address space randomization.	

	V-38597	🟥	🟨	🟩	▨	The system must limit the ability of processes to have simultaneous write and execute access to memory.	
	V-38600	🟥	🟨	🟩	▨	The system must not send ICMPv4 redirects by default.	
	V-38601	🟥	🟨	🟩	▨	The system must not send ICMPv4 redirects from any interface.	
	V-38605	🟥	🟨	🟩	▨	The cron service must be running.	
	V-38618	🟥	🟨	🟩	▨	The avahi service must be disabled.	
	V-38624	🟥	🟨	🟩	▨	System logs must be rotated daily.	
	V-38627	🟥	🟨	🟩	▨	The openldap-servers package must not be installed unless required.	
	V-38633	🟥	🟨	🟩	▨	The system must set a maximum audit log file size.	
	V-38634	🟥	🟨	🟩	▨	The system must rotate audit log files that reach the maximum file size.	
	V-38636	🟥	🟨	🟩	▨	The system must retain enough rotated audit logs to cover the required log retention period.	
	V-38642	🟥	🟨	🟩	▨	The system default umask for daemons must be 027 or 022.	
	V-38643	🟥	🟨	🟩	▨	There must be no world-writable files on the system.	
	V-38645	🟥	🟨	🟩	▨	The system default umask in /etc/login.defs must be 077.	
	V-38647	🟥	🟨	🟩	▨	The system default umask in /etc/profile must be 077.	
	V-38649	🟥	🟨	🟩	▨	The system default umask for the csh shell must be 077.	
	V-38651	🟥	🟨	🟩	▨	The system default umask for the bash shell must be 077.	
	V-38652	🟥	🟨	🟩	▨	Remote file systems must be mounted with the nodev option.	
	V-38653	🟥	🟨	🟩	▨	The snmpd service must not use a default	

		🟥	🟨	🟩	⬜	password.	
	V-38654	🟥	🟨	🟩	⬜	Remote file systems must be mounted with the nosuid option.	
	V-38656	🟥	🟨	🟩	⬜	The system must use SMB client signing for connecting to samba servers using smbclient.	
	V-38657	🟥	🟨	🟩	⬜	The system must use SMB client signing for connecting to samba servers using mount.cifs.	
	V-38660	🟥	🟨	🟩	⬜	The snmpd service must use only SNMP protocol version 3 or newer.	
	V-38668	🟥	🟨	🟩	⬜	The x86 Ctrl-Alt-Delete key sequence must be disabled.	
	V-38669	🟥	🟨	🟩	⬜	The postfix service must be enabled for mail delivery.	
	V-38671	🟥	🟨	🟩	⬜	The sendmail package must be removed.	
	V-38675	🟥	🟨	🟩	⬜	Process core dumps must be disabled unless needed.	
	V-38676	🟥	🟨	🟩	⬜	The xorg-x11-server-common (X Windows) package must not be installed unless required.	
	V-38679	🟥	🟨	🟩	⬜	The DHCP client must be disabled if not needed.	
	V-38681	🟥	🟨	🟩	⬜	All GIDs referenced in /etc/passwd must be defined in /etc/group	
	V-38693	🟥	🟨	🟩	⬜	The system must require passwords to contain no more than three consecutive repeating characters.	
	V-38697	🟥	🟨	🟩	⬜	The sticky bit must be set on all public directories.	
	V-38699	🟥	🟨	🟩	⬜	All public directories must be owned by a system account.	
	V-38701	🟥	🟨	🟩	⬜	The TFTP daemon must operate in secure mode which provides access only to a single directory on the host file system.	
	V-43150	🟥	🟨	🟩	⬜	The login user list must be disabled.	
	V-51337	🟥	🟨	🟩	⬜	The system must use a Linux Security Module at boot time.	

	V-51363	🟥	🟨	🟩	▨	The system must use a Linux Security Module configured to enforce limits on system services.	
	V-51369	🟥	🟨	🟩	▨	The system must use a Linux Security Module configured to limit the privileges of system services.	
	V-51379	🟥	🟨	🟩	▨	All device files must be monitored by the system Linux Security Module.	
	V-51391	🟥	🟨	🟩	▨	A file integrity baseline must be created.	
	V-51875	🟥	🟨	🟩	▨	The operating system upon successful logon/access must display to the user the number of unsuccessful logon/access attempts since the last successful logon/access.	
	V-54381	🟥	🟨	🟩	▨	The audit system must switch the system to single-user mode when available audit storage volume becomes dangerously low.	
CM-7 a	V-38587	🟥	🟨	🟩	▨	The telnet-server package must not be installed.	
	V-38591	🟥	🟨	🟩	▨	The rsh-server package must not be installed.	
	V-38603	🟥	🟨	🟩	▨	The ypserv package must not be installed.	
	V-38606	🟥	🟨	🟩	▨	The tftp-server package must not be installed unless required.	
	V-57569	🟥	🟨	🟩	▨	The noexec option must be added to the /tmp partition.	
CM-7 b	V-38478	🟥	🟨	🟩	▨	The Red Hat Network Service (rhnsd) service must not be running unless using RHN or an RHN Satellite.	
	V-38514	🟥	🟨	🟩	▨	The Datagram Congestion Control Protocol (DCCP) must be disabled unless required.	
	V-38515	🟥	🟨	🟩	▨	The Stream Control Transmission Protocol (SCTP) must be disabled unless required.	
	V-38516	🟥	🟨	🟩	▨	The Reliable Datagram Sockets (RDS) protocol must be disabled unless required.	
	V-38517	🟥	🟨	🟩	▨	The Transparent Inter-Process Communication (TIPC) protocol must be disabled unless required.	

	V-38582	🟥	🟨	🟩	⬜	The xinetd service must be disabled if no network services utilizing it are enabled.	
	V-38584	🟥	🟨	🟩	⬜	The xinetd service must be uninstalled if no network services utilizing it are enabled.	
	V-38604	🟥	🟨	🟩	⬜	The ypbind service must not be running.	
	V-38622	🟥	🟨	🟩	⬜	Mail relaying must be restricted.	
	V-38640	🟥	🟨	🟩	⬜	The Automatic Bug Reporting Tool (abrtd) service must not be running.	
	V-38641	🟥	🟨	🟩	⬜	The atd service must be disabled.	
	V-38644	🟥	🟨	🟩	⬜	The ntpdate service must not be running.	
	V-38646	🟥	🟨	🟩	⬜	The oddjobd service must not be running.	
	V-38648	🟥	🟨	🟩	⬜	The qpidd service must not be running.	
	V-38650	🟥	🟨	🟩	⬜	The rdisc service must not be running.	
	V-38672	🟥	🟨	🟩	⬜	The netconsole service must be disabled unless required.	
CM-8 (3) (a)	V-38696	🟥	🟨	🟩	⬜	The operating system must employ automated mechanisms per organization defined frequency to detect the addition of unauthorized components/devices into the operating system.	
CP-9 (a)	V-38488	🟥	🟨	🟩	⬜	The operating system must conduct backups of user-level information contained in the operating system per organization defined frequency to conduct backups consistent with recovery time and recovery point objectives.	
CP-9 (b)	V-38486	🟥	🟨	🟩	⬜	The operating system must conduct backups of system-level information contained in the information system per organization defined frequency to conduct backups that are consistent with recovery time and recovery point objectives.	
IA-11	V-58901	🟥	🟨	🟩	⬜	The sudo command must require authentication.	
IA-2	V-38460	🟥	🟨	🟩	⬜	The NFS server must not have the all_squash option enabled.	
	V-38492	🟥	🟨	🟩	⬜	The system must prevent the root account from	

						logging in from virtual consoles.	
	V-38677					The NFS server must not have the insecure file locking option enabled.	
IA-2 (1)	V-38595					The system must be configured to require the use of a CAC PIV compliant hardware token or Alternate Logon Token (ALT) for authentication.	
IA-2 (2)	V-38611					The SSH daemon must ignore .rhosts files.	
	V-38612					The SSH daemon must not allow host-based authentication.	
	V-38614					The SSH daemon must not allow authentication using an empty password.	
IA-2 (5)	V-38494					The system must prevent the root account from logging in from serial consoles.	
	V-38613					The system must not permit root logins using remote access programs such as ssh.	
IA-2 (8)	V-38607					The SSH daemon must be configured to use only the SSHv2 protocol.	
IA-2 (9)	V-38626					The LDAP client must use a TLS connection using trust certificates signed by the site CA.	
IA-4 e	V-38694					The operating system must manage information system identifiers for users and devices by disabling the user identifier after an organization defined time period of inactivity.	
IA-5 (1) (a)	V-38475					The system must require passwords to contain a minimum of 15 characters.	
	V-38482					The system must require passwords to contain at least one numeric character.	
	V-38569					The system must require passwords to contain at least one uppercase alphabetic character.	
	V-38570					The system must require passwords to contain at least one special character.	
	V-38571					The system must require passwords to contain at least one lowercase alphabetic character.	

IA-5 (1) (b)	V-38572	🟥	🟨	🟩	▨	The system must require at least eight characters be changed between the old and new passwords during a password change.	
IA-5 (1) (d)	V-38477	🟥	🟨	🟩	▨	Users must not be able to change passwords more than once every 24 hours.	
	V-38479	🟥	🟨	🟩	▨	User passwords must be changed at least every 60 days.	
IA-5 (1) c	V-38619	🟥	🟨	🟩	▨	There must be no .netrc files on the system.	
IA-5 (1) e	V-38658	🟥	🟨	🟩	▨	The system must prohibit the reuse of passwords within five iterations.	
IA-7	V-38574	🟥	🟨	🟩	▨	The system must use a FIPS 140-2 approved cryptographic hashing algorithm for generating account password hashes (system-auth).	
	V-38576	🟥	🟨	🟩	▨	The system must use a FIPS 140-2 approved cryptographic hashing algorithm for generating account password hashes (login.defs).	
	V-38577	🟥	🟨	🟩	▨	The system must use a FIPS 140-2 approved cryptographic hashing algorithm for generating account password hashes (libuser.conf).	
IA-8	V-38683	🟥	🟨	🟩	▨	All accounts on the system must have unique user or account names	
MA-4	V-38589	🟥	🟨	🟩	▨	The telnet daemon must not be running.	
MA-4 e	V-38610	🟥	🟨	🟩	▨	The SSH daemon must set a timeout count on idle sessions.	
MP-4 (1)	V-38659	🟥	🟨	🟩	▨	The operating system must employ cryptographic mechanisms to protect information in storage.	
RA-5	V-38489	🟥	🟨	🟩	▨	A file integrity tool must be installed.	
RA-5 (7)	V-38698	🟥	🟨	🟩	▨	The operating system must employ automated mechanisms to detect the presence of unauthorized software on organizational information systems and notify designated organizational officials in accordance with the organization defined frequency.	

SA-7	V-38483	🟥	🟨	🟩	▨	The system package management tool must cryptographically verify the authenticity of system software packages during installation.	
SA-7	V-38487	🟥	🟨	🟩	▨	The system package management tool must cryptographically verify the authenticity of all software packages during installation.	
SC-10	V-38608	🟥	🟨	🟩	▨	The SSH daemon must set a timeout interval on idle sessions.	
SC-13	V-38617	🟥	🟨	🟩	▨	The SSH daemon must be configured to use only FIPS 140-2 approved ciphers.	
SC-28	V-38661	🟥	🟨	🟩	▨	The operating system must protect the confidentiality and integrity of data at rest.	
SC-28 (1)	V-38662	🟥	🟨	🟩	▨	The operating system must employ cryptographic mechanisms to prevent unauthorized disclosure of data at rest unless otherwise protected by alternative physical measures.	
SC-5 (2)	V-38539	🟥	🟨	🟩	▨	The system must be configured to use TCP syncookies when experiencing a TCP SYN flood.	
SC-7	V-38512	🟥	🟨	🟩	▨	The operating system must prevent public IPv4 access into an organizations internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.	
	V-38549	🟥	🟨	🟩	▨	The system must employ a local IPv6 firewall.	
	V-38551	🟥	🟨	🟩	▨	The operating system must connect to external networks or information systems only through managed IPv6 interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	
	V-38553	🟥	🟨	🟩	▨	The operating system must prevent public IPv6 access into an organizations internal networks except as appropriately mediated by managed interfaces employing boundary protection	

		🟥	🟨	🟩	▨	devices.	
	V-38555	🟥	🟨	🟩	▨	The system must employ a local IPv4 firewall.	
SC-7 (5)	V-38686	🟥	🟨	🟩	▨	The systems local firewall must implement a deny-all allow-by-exception policy for forwarded packets.	
SC-7 c	V-38560	🟥	🟨	🟩	▨	The operating system must connect to external networks or information systems only through managed IPv4 interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	
SC-9	V-38687	🟥	🟨	🟩	▨	The system must provide VPN connectivity for communications over untrusted networks.	
SI-11 b	V-38518	🟥	🟨	🟩	▨	All rsyslog-generated log files must be owned by root.	
	V-38519	🟥	🟨	🟩	▨	All rsyslog-generated log files must be group-owned by root.	
	V-38623	🟥	🟨	🟩	▨	All rsyslog-generated log files must have mode 0600 or less permissive.	
SI-2 (2)	V-38481	🟥	🟨	🟩	▨	System security patches and updates must be installed and up-to-date.	
SI-3	V-38666	🟥	🟨	🟩	▨	The system must use and update a DoD-approved virus scan program.	
SI-4 (5)	V-38667	🟥	🟨	🟩	▨	The system must have a host-based intrusion detection tool installed.	
	V-38700	🟥	🟨	🟩	▨	The operating system must provide a near real-time alert when any of the organization defined list of compromise or potential compromise indicators occurs.	
SI-7	V-38670	🟥	🟨	🟩	▨	The operating system must detect unauthorized changes to software and information.	